JOURNAL OF ALGEBRA 53, 389–394 (1978)

Existenz und Konjugiertsein von Untergruppen, die in endlichen auflösbaren Gruppen durch gewisse Indexschranken definiert sind

WOLFGANG GASCHÜTZ

Mathematisches Seminar der Universität, 23 Kiel, Deutschland

Communicated by B. Huppert

Received October 17, 1977

Ziel dieser Note ist der Beweis der folgenden allgemeinen Eigenschaft endlicher auflösbarer Gruppen:

1. SATZ. *Sei $n \in \mathbb{N}$ und G eine endliche auflösbare Gruppe. Dann gilt:*

(a) *In G existiert eine Untergruppe H, die*

$$S <_{\max} H \Rightarrow H : S \leqslant n$$

und

$$H \leqslant S <_{\max} L \leqslant G \Rightarrow L : S > n$$

erfüllt.

(b) *Alle gemäss* (a) *existierenden H sind unter G konjugiert.*

Dabei bedeute wie auch allgemein $X <_{\max} Y$, dass X maximale Untergruppe von Y ist.

Hat H die Eigenschaften (a) des Satzes 1, so hat offenbar auch jede zu H unter G konjugierte Untergruppe diese Eigenschaften.

Da in endlichen auflösbaren Gruppen maximale Untergruppen stets Primzahlpotenzindex haben, sind in Satz 1 unter den n nur die Primzahlpotenzen relevant.

Offenbar kann in der zweiten Eigenschaft unter (a) anstelle von $S <_{\max} L$ auch $S < L$ gesetzt werden.

Wir beweisen 1 durch Anwendung der in [2, 4] entwickelten Mechanismen. Dazu erinnern wir zunächst an die Eigenschaften einer primitiven endlichen auflösbaren Gruppe; s. [3, II.3.2, 3.3, und 3.8]: Sei allgemein $\mathrm{Cor}_X Y$ für $Y \leqslant X$ der grösste Normalteiler von X, der in Y enthalten ist; also $\mathrm{Cor}_X Y = \bigcap_{x \in X} Y^x$. Eine Gruppe J heisse primitiv, wenn $S <_{\max} J$ existiert mit $\mathrm{Cor}_J S = 1$.

0021-8693/78/0532-0389$02.00/0
Copyright © 1978 by Academic Press, Inc.
All rights of reproduction in any form reserved.

Primitivsein bedeutet also kurz die Existenz einer treuen primitiven Permutationsdarstellung. J ist genau dann eine primitive endliche auflösbare Gruppe, wenn J semidirektes Produkt einer elementar-abelschen Gruppe M mit einer endlichen auflösbaren Gruppe S ist, zu einem Monomorphismus von S in die Automorphismengruppe von M, durch den S irreduzibel auf M operiert; s. [3, I.14.4]. Hierbei ist M einziger minimaler Normalteiler von J; M ist komplementierbar in J und alle seine Komplemente sind unter M zu S konjugiert. Für primitive endliche auflösbare J setzen wir grad $J = J{:}S = |M|$. Dann ist grad J also der Grad der einzigen treuen primitiven Permutationsdarstellung von J.

Weiterhin komprimieren wir zur besseren Anwendbarkeit die für uns wichtigen Resultate aus [4] in dem folgenden

2. Satz. *Sei $\mathfrak{J}$ eine Klasse primitiver endlicher auflösbarer Gruppen mit der Eigenschaft, dass mit J auch jedes primitive epimorphe Bild von J zu $\mathfrak{J}$ gehört. Sei ferner G eine endliche auflösbare Gruppe.*

Dann gilt:

(a) *In G existiert eine Untergruppe H, die*

$$S <_{\max} H \Rightarrow H/\mathrm{Cor}_H\, S \in \mathfrak{J}$$

und

$$H \leqslant S <_{\max} L \leqslant G \Rightarrow L/\mathrm{Cor}_L\, S \notin \mathfrak{J}$$

erfüllt.

(b) *Alle gemäss* (a) *existierenden H sind unter G konjugiert.*

Beweis. Sei $\mathfrak{H}$ die Klasse aller endlichen auflösbaren Gruppen, deren primitive Faktorgruppen alle zu $\mathfrak{J}$ gehören. (Hierbei ist eigentlich die Forderung der Auflösbarkeit unnötig, da mit allen primitiven Faktorgruppen einer endlichen Gruppe auch die Faktorgruppe nach der Frattinigruppe auflösbar und allgemein die Frattinigruppe nilpotent ist.) Offenbar ist $\mathfrak{H}$ in der Bezeichnungsweise von [4, 3.1 und 4.2] ein Homomorph und gleich seinem gesättigten Abschluss.

Wir zeigen, dass die Gruppe H mit den Eigenschaften (a) eine im Sinne von [4, 3.2] zugehörige $\mathfrak{H}$-Untergruppe von G ist. Dann folgt der Satz aus [4, 4.4].

$H \in \mathfrak{H}$: Sei H/N irgendeine primitive Faktorgruppe von H, also etwa $S <_{\max} H$ mit $\mathrm{Cor}_H\, S = N$. Dann ist nach Voraussetzung $H/N \in \mathfrak{J}$. Nach der Definition von $\mathfrak{H}$ ist also $H \in \mathfrak{H}$.

Sei $H \leqslant L \leqslant G$ und $L_0 \leqslant L$. Ist $L_0 H \leqslant S <_{\max} L$, so ist $L/\mathrm{Cor}_L\, S \notin \mathfrak{J}$ nach Voraussetzung und $L/L_0 \notin \mathfrak{H}$ nach der Definition von $\mathfrak{H}$. Also folgt $L_0 H = L$ aus $L/L_0 \in \mathfrak{H}$. Q.E.D.

Wir kommen nun zur Konstruktion der speziellen Klasse $\mathfrak{J}$, mit der wir durch

Anwendung des Satzes 2 den Satz 1 gewinnen wollen. Dies erfordert einige weitere Vorbereitungen.

Sei X eine Gruppe und q eine Primzahl. Dann sei die q-Breite von X definiert durch

$$b_q(X) = \sup\{\beta \mid Z \leqslant Y \leqslant X,\ Y/Z \text{ elementar-abelsche } q\text{-Gruppe},\ Y{:}Z = q^\beta\}.$$

$b_q(X)$ verhält sich offenbar beim Übergang zu Untergruppen von X monoton fallend. Es gilt auf Grund des Isomorphiesatzes $b_q(X) \leqslant b_q(X/Y) + b_q(Y)$ für $Y \leqslant X$. Ist $X \wr Y$ das reguläre Kranzprodukt von X mit Y, so erhält man durch iterierte Anwendung dieser Regel $b_q(X \wr Y) \leqslant |Y|\, b_q(X) + b_q(Y)$; s. [3, I. 15.6]. Ferner ist trivialerweise $b_q(X) = b_q(Q)$ für eine q-Sylowgruppe Q von X.

3. Satz. *Seien p und q Primzahlen, $p \neq q$, M eine elementar-abelsche Gruppe der Ordnung p^m und Q eine q-Sylowgruppe der Automorphismengruppe von M.*

Dann gilt $q^{b_q(Q)} < p^m$.

Beweis. Die in Rede stehende Autormophismengruppe ist isomorph zur Gruppe $GL(m, p)$. Wir bedienen uns der Beschreibungen von Q durch Weir [5] für $q \neq 2$ sowie Carter und Fong [1] für $q = 2$. $\mathbb{Z}_a$ bzw. $\tilde{\mathbb{D}}_{2^\alpha}$ bezeichnet allgemein die zyklische Gruppe der Ordnung a bzw. die Quasidiedergruppe der Ordnung 2^α; s. [3, I.14.9].

Fall $q \neq 2$: Sei e minimal mit $p^e \equiv 1 \bmod q$, $p^e - 1 = q^r k$ mit $q \nmid k$, $m = c + ea$ mit $0 \leqslant c < e$ und $a = a_0 + a_1 q + \cdots$ in q-adischer Entwicklung. Sei ferner $Q_0 = \mathbb{Z}_{q^r}$ und rekursiv $Q_{i+1} = Q_i \wr \mathbb{Z}_q$ für $i \geqslant 0$.

Dann ist $Q = Q_0^{a_0} \times Q_1^{a_1} \times \cdots$, wobei hier wie auch später durch die Exponenten a_i das a_i-fache direkte Produkt der Basisgruppe Q_i gemeint sei.

Fall $q = 2$: Sei $m = 2^{i_0} + 2^{i_1} + \cdots$, $i_0 < i_1 < \cdots$.

Für $p \equiv 1 \bmod 4$ sei $p - 1 = 2^r k$, $2 \nmid k$; ferner $Q_0 = \mathbb{Z}_{2^r}$ und rekursiv $Q_{i+1} = Q_i \wr \mathbb{Z}_2$ für $i \geqslant 0$.

Dann ist $Q = Q_{i_0} \times Q_{i_1} \times \cdots$.

Für $p \equiv 3 \bmod 4$ sei $p + 1 = 2^s l$, $2 \nmid l$; ferner $Q_0 = \mathbb{Z}_2$, $Q_1 = \tilde{\mathbb{D}}_{2^{s+2}}$ und rekursiv $Q_{i+1} = Q_i \wr \mathbb{Z}_2$ für $i \geqslant 1$.

Dann ist $Q = Q_{i_0} \times Q_{i_1} \times \cdots$.

Wir schätzen nun $q^{b_q(Q)}$ mit den vorangeschickten Bemerkungen über die q-Breite ab:

Fall $q \neq 2$: Zunächst ergibt sich leicht mit Induktion

$$q^{b_q(Q_i)} \leqslant q^{1+q+\cdots+q^i} < q^{(q/(q-1))q^i} \qquad \text{für } i \geqslant 0.$$

Für $r = 1$ gilt noch etwas schärfer $q^{b_q(Q_0)} = q$ und $q^{b_q(Q_1)} \leqslant q^q$, da $|Q_1| = |\mathbb{Z}_q \wr \mathbb{Z}_q| = q^{1+q}$ aber Q_1 nicht abelsch ist; mit Induktion erhält man jetzt

$$q^{b_q(Q_i)} \leqslant q^{1+q+\cdots+q^{i-2}+q^i} = q^{q^i((1/q^i)(q^{i-1}-1)/(q-1)+1)} \qquad \text{für } i \geqslant 2.$$

Es ist dann also

$$q^{b_q(Q_i)} < (q^{1/q(q-1)+1})^{q^i} \qquad \text{für } i \geqslant 0.$$

Nun ist $q < 2^{q-1} < ((1 + 1/q)^q)^{q-1}$, d.h. $q^{1/q(q-1)+1} < 1 + q$. Ist $r = 1$, so gilt also $q^{b_q(Q_i)} < (1 + q)^{q^i}$ für $i \geqslant 0$. Es ist $q \mid 2^{q-1} - 1$, also $q < 2^{q-1}$ und $q^{1/(q-1)} < 2$. Ferner ist $q^r \mid p^e - 1$; also ist $2q \leqslant p^e - 1 < p^e$ oder es ist $p = 2$, $q = 2^e - 1$ und $r = 1$.

Im ersten Fall ist

$$q^{b_q(Q)} \leqslant q^{(q/(q-1))a} = q^{(1/(q-1))a+a} \leqslant 2^a q^a < p^{ea} \leqslant p^m.$$

Im zweiten Fall ist

$$q^{b_q(Q)} < (1 + q)^a = 2^{ea} \leqslant p^m.$$

Fall $q = 2$, $p \equiv 1 \bmod 4$: Jetzt ergibt sich mit Induktion

$$2^{b_2(Q_i)} \leqslant 2^{2^{i+1}-1} \qquad \text{für } i \geqslant 0$$

und daher

$$2^{b_2(Q)} \leqslant 2^{2^{i_0+1}-1} 2^{2^{i_1+1}-1} \cdots < 2^{2(2^{i_0}+2^{i_1}+\cdots)} < 5^m \leqslant p^m.$$

Fall $q = 2$, $p \equiv 3 \bmod 4$: Jetzt ist $2^{b_2(Q_0)} = 2$, $2^{b_2(Q_1)} = 2^2$ und dann mit Induktion

$$2^{b_2(Q_i)} \leqslant 2\, 2^2 \cdots 2^{2^{i-2}} 2^{2^i} = 2^{2^{i-1}-1+2^i} < (2^{3/2})^{2^i} < 3^{2^i},$$

zunächst für $i \geqslant 1$, aber offenbar auch für $i = 0$ und daher

$$2^{b_2(Q)} < 3^{2^{i_0}+2^{i_1}+\cdots} < p^m.$$

4. SATZ. *Sei M eine elementar-abelsche Gruppe der Ordnung p^m, p Primzahl, und S eine auf M treu und irreduzibel operierende auflösbare Gruppe von Automorphismen. K/L. sei ein Hauptfaktor von S, $\mid K/L \mid = q^\beta$, q Primzahl.*

Dann gilt $q^\beta < p^m$.

Beweis. Zunächst sei daran erinnert, dass die Ordnung des maximalen nilpotenten Normalteilers von S zu p teilerfremd ist; s. [3, II.3.2.e].

Wir wenden vollständige Induktion nach $\mid L \mid$ an.

Ist $p \neq q$ so folgt der Satz sofort aus 3. Insbesondere gilt er also für $\mid L \mid = 1$ nach der zu Beginn des Beweises erfolgten Erinnerung.

Da $p = q$ zufolge K nicht im maximalen nilpotenten Normalteiler von S liegt, zentralisiert K nicht alle Hauptfaktoren von S unterhalb von L. Sei

$M_0 = K^*/L^*$ ein von K nicht zentralisierter Hauptfaktor von S mit $K^* \leqslant L$. Dann ist $L^* < L$. Ist $|M_0| = p_0^{m_0}$, so folgt mit Induktion zunächst $p_0^{m_0} < p^m$. Ist $C = C_S(M_0)$ der in S gebildete Zentralisator von M_0, so ist K/L in natürlicher Weise mit dem Hauptfaktor KC/LC von $S_0 = S/C$ isomorph. Hierbei ist

$$|LC/C| = |L/L \cap C| \leqslant |L/K^*| < L.$$

S_0 operiert in natürlicher Weise treu und irreduzibel auf M_0. Mit erneuter Anwendung der Induktion ist nun $q^\beta < p_0^{m_0}$ und mit der vorher festgestellten Ungleichung $q^\beta < p^m$.

5. KOROLLAR. *Sei J eine primitive endliche auflösbare Gruppe und J^φ ein primitives epimorphes Bild von J.*

Dann ist grad $J^\varphi \leqslant$ grad J. *Für $n \in \mathbb{N}$ erfüllt die Klasse $\mathfrak{J}$ der primitiven endlichen auflösbaren Gruppen J mit* grad $J \leqslant n$ *also die Voraussetzungen des Satzes* 2.

Beweis. Es darf $|J^\varphi| < |J|$ angenommen werden.

Ist M der minimale Normalteiler von J und S ein Komplement von M in J, so ist $|J^\varphi| < |J|$ zufolge J^φ in natürlicher Weise epimorphes Bild von S und der minimale Normalteiler von J^φ zu einem Hauptfaktor K/L von S isomorph. Da grad $J = |M|$ und grad $J^\varphi = |K/L|$ ist, folgt nun der Satz aus **4**.

Beweis von 1. Es sei $\mathfrak{J}$ wie in 5.

Wir müssen noch zeigen, dass die Aussagen des Satzes 2 für dieses spezielle $\mathfrak{J}$ die Aussagen des Satzes 1 liefern:

(a) $H/\mathrm{Cor}_H\, S \in \mathfrak{J}$ bedeutet $\mathrm{grad}(H/\mathrm{Cor}_H\, S) \leqslant n$, also $(H/\mathrm{Cor}_H\, S):(S/\mathrm{Cor}_H\, S) = H{:}S \leqslant n$.

(b) $L/\mathrm{Cor}_L\, S \notin \mathfrak{J}$ bedeutet $\mathrm{grad}(L/\mathrm{Cor}_L\, S) > n$, also $(L/\mathrm{Cor}_L\, S):(S/\mathrm{Cor}_L\, S) = L{:}S > n$. Q.E.D.

Herr K. Johnson wies mich freundlicherweise auf eine Formulierung von Satz **4** hin, die wir abschliessend angeben wollen; die Aquivalenz der beiden Aussagen wird der Leser leicht selbst bestätigen können.

6. KOROLLAR. *Sei G eine endliche auflösbare Gruppe und K/L ein Hauptfaktor von G mit maximaler Ordnung.*

Dann ist K im maximalen nilpotenten Normalteiler von G enthalten.

LITERATUR

1. R. W. CARTER UND P. FONG, The Sylow 2-subgroups of the finite classical groups, *J. Algebra* **1** (1964), 139–151.

2. W. Gaschütz, Zur Theorie der endlichen auflösbaren Gruppen, *Math. Z.* **80** (1963), 300–305.
3. B. Huppert, "Endliche Gruppen I," Springer, Berlin/Heidelberg/New York, 1967.
4. H. Schunck, $\mathfrak{H}$-Untergruppen in endlichen auflösbaren Gruppen, *Math. Z.* **97** (1967), 326–330.
5. A. Weir, Sylow p-subgroups of the general linear groups over fields of characteristic p, *Proc. Amer. Math. Soc.* **6** (1955), 529–533.